Vulnerability & Patch Management
Questions Board Members Should Ask

Below are some questions you may ask management to ensure appropriate, comprehensive vulnerability and patch management practices have been implemented to protect against cyber threats.

1. ***What resources are leveraged to understand the nature of threats to the institution? Does the institution receive ongoing threat information from reliable sources, such as FS-ISAC, US-CERT, NIST, regulatory and law enforcement alerts, and trusted vendor partners? Does the institution maintain an ongoing process to periodically scan systems and software for vulnerabilities?***

   WHY THIS IS IMPORTANT: To help the institution better understand the nature of threats, it is important to integrate relevant threat information into the vulnerability management program. This can be accomplished through the ***monitoring of third-party information sources****, such as FS-ISAC, US-CERT, NIST, and regulatory and law enforcement alerts. Threat information from these third-party sources should ideally be integrated into the institution's asset scanning programs. The FFIEC's Information Technology Handbook booklet, Architecture, Infrastructure, and Operations, states that "****management should implement a process to periodically assess systems and software for vulnerabilities using scanners that are updated with a current vulnerability list".*** The effectiveness of scanning efforts is dependent on the existence of a comprehensive asset inventory of approved systems, software, and devices, and *scans should include all systems and software in the institution's hardware, software, and telecommunications inventories. Proper controls, including separation of duties, logical security, configuration management, and log review should be in place to protect these scanning tools against unauthorized use or access to sensitive information.*[1] Scans should ideally be agent-based or authenticated for higher-confidence results.

2. ***Does the institution have an established process for identifying available software and hardware patches, and does the institution actively evaluate those patches against the threat and network environment?***

   WHY THIS IS IMPORTANT: Patches for software and hardware assets, including patches to address critical security vulnerabilities, are released frequently. This process should be timely and present a comprehensive view of available patches that refreshes frequently as new patches are introduced. In addition, available patches should be evaluated against the institution's threat and network environment. This process will allow the institution to tailor the application of patches to its own unique environment and will assist in the prioritization of patches by severity and potential impact to the institution.[2]

3. ***Does the institution have a process to address the prioritization of patches that identifies which patches to apply across classes of computers and applications? Is there a process for obtaining, testing, and securely installing patches, including those applicable to the institution's virtual environment?***

[1] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - VI.B.3- Vulnerability and Patch Management. June 2021.
[2] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security - II.C..10(d) - Patch Management. September 2016.

WHY THIS IS IMPORTANT: ***Patches should ideally be prioritized based upon severity****, with Known Exploited Vulnerabilities (KEVs), critical, and high-severity patches receiving the most urgent priority in the institution's patching regimen.* ***CISA notes that "critical" vulnerabilities should be remediated within 15 calendar days of initial detection; "high" severity vulnerabilities should be remediated within 30 calendar days.***[3] *Institutions should also be aware of smaller remediation windows that may be recommended by vendors to remediate more urgent vulnerabilities. In the event a vendor fails to assign a rating to a specific vulnerability, the institution should perform internal threat modeling or consult external sources, such as FS-ISAC, to determine prioritization for remediating the vulnerability.*

Once the institution has identified and prioritized necessary patches, it is necessary to retrieve patches from the vendor. Testing patches in a controlled, non-production environment can more safely reveal how changes to a patched asset might interact with or create conflicts in the operating environment prior to enterprise-wide deployment.[4]

4. ***Does the institution actively track any patches or security updates that management chooses to delay or not apply? Is there a process to document and track these exceptions? Have sufficient compensating controls been applied to any unpatched assets that exist within the institution?***

   WHY THIS IS IMPORTANT: There are occasionally circumstances where patches may not be readily applicable within the institution's environment (e.g., when unacceptable interoperability conflicts occur, etc.). Documenting and tracking unapplied patches can help management understand the nature of any issues noted, as well as any necessary plans for remediation, including the application of compensating controls, until issues can be resolved.[5]

5. ***Does the institution ensure that any patches applied in the production environment are also applied in the disaster recovery environment in a timely manner? Is there a documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied?***

   WHY THIS IS IMPORTANT: The institution should ensure that all patches installed in the production environment are mirrored in the disaster recovery environment to ensure security and consistency should a failover become necessary. In addition, patching can introduce new features, updated version numbers, changes to dependencies, or even compatibility issues within the institution's environment. Documentation of patch changes can help to ensure that the institution is fully aware of the current state of its inventory and that its disaster recovery plans are reflective of the current state of assets in the environment.[6]

[3] CISA. *CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems*.
[4] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security - II.C..10(d) - Patch Management. September 2016.
[5] Ibid.
[6] Ibid.